

¿Puede Cyber Crucible detener el movimiento lateral del atacante?

El motor de comportamiento del producto y las metodologías de Zero Trust recopilan eficazmente evidencia de movimiento lateral.

Esa evidencia puede ser de movimiento lateral de proceso a proceso en la propia máquina, o puede tratarse del descubrimiento del punto de entrada de un atacante al sistema desde un sistema remoto, durante la realización de un Análisis de Causa Raíz.

Los programas y sus argumentos asociados con métodos de inyección de procesos y procesos de “living off the land” que abren otros procesos son capturados y enviados a Cyber Crucible.

Debido a la analítica de comportamiento de procesos a nivel de kernel, no existen procesos demasiado privilegiados para la observación y notificación de Cyber Crucible (incluyendo otros controladores de kernel, o incluso otras herramientas de seguridad de endpoint).

Las respuestas automatizadas de contra-extorsión se producen cuando se inician acciones de extorsión de datos o de cifrado por ransomware.

Por ejemplo, aquí se muestra un video que demuestra el movimiento lateral a través de una máquina, utilizando técnicas en memoria, y el exploit de Log4J. Tenga en cuenta que la suspensión automatizada del/los proceso(s) afectado(s) ocurrió después de que se iniciaran comportamientos de robo de datos y ransomware.

[rr-log4j-procinj-3mins.mp4](#)

Otro ejemplo de esta dinámica demuestra el uso por parte de un atacante para abrir un shell de Windows. La observación capturó toda la evidencia, pero la actividad fue suspendida una vez que el shell de Windows comenzó a intentar actividades de extorsión de datos (en este caso, robo de datos)

[rr-com-dll.mp4](#)

Por último, también se observa la migración desde un navegador explotado, y en este caso el atacante nunca logró moverse con éxito desde el navegador Chrome explotado, debido al monitoreo del estado de memoria del navegador:

[rr-untrusted-chrome.mp4](#)

Revision #1

Created 2026-07-24 01:39:42 UTC by Dennis Underwood

Updated 2026-07-24 01:39:42 UTC by Dennis Underwood